

**FINAL EVALUATION REPORT**  
**CISCO SYSTEMS, INC.**  
**CISCO PIX FIREWALL 520 VERSION 4.3(1)**

**FINAL**  
**JANUARY 1999**

**PREPARED BY:**  
**COMPUTER SCIENCES CORPORATION**  
**7471 CANDLEWOOD ROAD**  
**HANOVER, MD 21076**

**PREPARED FOR:**  
**CISCO SYSTEMS, INC.**  
**380 HERNDON PARKWAY**  
**SUITE 300**  
**HERNDON, VA 20170**

**SUBMITTED TO:**  
**TTAP OVERSIGHT BOARD**  
**9800 SAVAGE RD**  
**FT. MEADE, MD 20755**

**APPROVED FOR PUBLIC RELEASE;**  
**DISTRIBUTION UNLIMITED**

## FOREWORD

This publication, the Cisco Systems PIX Firewall Final Evaluation Report, is being issued by Computer Sciences Corporation. This report is the principle source of information used by the Trust Technology Assessment Program (TTAP) Oversight Board to render a certification rating for the Cisco PIX Firewall. It is intended to support the TTAP certification process by providing all the information needed by the TTAP Oversight Board to verify the results of the evaluation. This report presents all evaluation results, their justifications, and any findings derived from the work performed during the evaluation. The requirements stated in this report are taken from the *Cisco PIX Firewall 520 Version 4.3(1) Security Target* and conformant with the *Common Criteria for Information Technology Security Evaluation*, Version 2.0.

## ACKNOWLEDGEMENTS

### Evaluation Team Members

#### *Computer Sciences Corporation*

Kimberly Caplan

H. Patrick Dunn

Kim Jones

Barbara Mayer

Vince Ritts

#### *National Security Agency*

Jack Walsh

With special thanks to Carl Souba

## TABLE OF CONTENTS

<b>FOREWORD .....</b>	<b>i</b>
<b>ACKNOWLEDGEMENTS.....</b>	<b>ii</b>
<b>Executive Summary .....</b>	<b>1</b>
<b>1.0 Introduction.....</b>	<b>2</b>
1.1 BACKGROUND.....	2
1.2 DOCUMENT ORGANIZATION.....	2
<b>2.0 Identification .....</b>	<b>4</b>
2.1 EVALUATED CONFIGURATION.....	4
2.2 SYSTEM OVERVIEW .....	5
2.3 HARDWARE OVERVIEW .....	7
2.4 SOFTWARE OVERVIEW.....	7
2.4.1 PIX Firewall Software Components .....	8
2.4.2 NT Workstation Software Components .....	9
<b>3.0 Security Policy.....</b>	<b>10</b>
<b>4.0 Assumptions and Clarification of Scope.....</b>	<b>12</b>
4.1 USAGE ASSUMPTIONS.....	12
4.2 ENVIRONMENTAL ASSUMPTIONS.....	12
4.3 CLARIFICATION OF SCOPE.....	12
<b>5.0 Documentation .....</b>	<b>13</b>
<b>6.0 Product Testing.....</b>	<b>14</b>
6.1 TOE CONFIGURATIONS USED IN TESTING .....	14
6.2 RESULTS OF DEVELOPER TESTING.....	16
6.3 RESULTS OF EVALUATOR TESTING .....	16
<b>7.0 Results of the TOE Evaluation.....</b>	<b>18</b>
7.1 TOE SECURITY REQUIREMENTS.....	18
7.2 EVALUATION APPROACH .....	19
7.3 REQUIREMENT VERIFICATION .....	20
7.3.1 Configuration Management .....	20
7.3.2 Delivery and Operation .....	20
7.3.3 Development .....	21
7.3.4 Guidance Documents.....	22
7.3.5 Tests.....	22
7.3.6 Vulnerability Assessment .....	24
7.4 FUNCTIONAL REQUIREMENT SATISFACTION .....	25
7.4.1 FMT_SMR.1 Security roles.....	25
7.4.2 FIA_ATD.1 User attribute definition.....	25
7.4.3 FIA_UID.2 User identification before any action .....	26

7.4.4	<i>FIA_UAU.1 Timing of authentication.....</i>	26
7.4.5	<i>FDP_IFC.1 Subset information flow control .....</i>	27
7.4.6	<i>FDP_IFF.1 Simple security attributes.....</i>	27
7.4.7	<i>FMT_MSA.3 Static attribute initialization.....</i>	29
7.4.8	<i>FDP_RIP.2 Full residual information protection.....</i>	30
7.4.9	<i>FPT_RVM.1 Non-bypassability of the TSP.....</i>	30
7.4.10	<i>FPT_SEP.1 TSF domain separation.....</i>	31
7.4.11	<i>FPT_STM.1 Reliable timestamps .....</i>	32
7.4.12	<i>FAU_GEN.1 Audit data generation.....</i>	32
7.4.13	<i>FAU_SAR.1 Audit review.....</i>	35
7.4.14	<i>FAU_SAR.3 Selectable audit review.....</i>	36
7.4.15	<i>FAU_STG.1 Protected audit trail storage .....</i>	36
7.4.16	<i>FAU_STG.4 Prevention of audit data loss.....</i>	37
7.4.17	<i>FMT_MOF.1 Management of security functions behavior .....</i>	37
<b>8.0</b>	<b>Evaluator Comments .....</b>	<b>40</b>
8.1	AUDIT REVIEW TOOL .....	40
8.2	AUDITABLE EVENTS .....	40
8.3	TOE ARCHITECTURE.....	40
8.4	ASYMMETRIC RULES FOR POLICY ENFORCEMENT.....	40
8.5	USE OF PROCEDURES TO AVOID CONTRADICTIONARY AUDIT MESSAGE.....	40
<b>9.0</b>	<b>Glossary.....</b>	<b>41</b>
<b>10.0</b>	<b>Bibliography .....</b>	<b>42</b>
<b>Appendix A – Security Target.....</b>		<b>A-1</b>
<b>Appendix B - Evaluated Configuration Parameters and Files .....</b>		<b>B-1</b>

## LIST OF TABLES

Table 1 TOE Identification.....	4
Table 2 TOE Components for Testing .....	14
Table 3 TOE Functional Requirements.....	18
Table 4 TOE Assurance Requirements .....	19
Table 5 Test Coverage of Security Functional Requirements .....	23
Table 6 TOE Audit Events .....	34

## LIST OF FIGURES

Figure 1 Evaluated Configuration.....	5
Figure 2 TOE Test Configuration .....	15
Figure 3 Auditable Events .....	33

## Executive Summary

This document describes the results of Trust Technology Assessment Program (TTAP) evaluation of the security protection provided by the Cisco PIX Firewall 520 Version 4.3(1) configured as described in the *Cisco PIX Firewall 520 Version 4.3(1) Installation and Configuration White Paper*. This product was examined by Computer Sciences Corporation in cooperation with Cisco Systems personnel. The security features of the Cisco PIX Firewall were examined against the requirements specified in the *Cisco PIX Firewall 520 Version 4.3(1) Security Target* in order to establish a candidate rating.

The version of the product evaluated was Cisco PIX Firewall 520 Version 4.3(1). This product is also described in this report as the Target of Evaluation (TOE). The developer for the product was Cisco Systems Incorporated. The PIX Firewall is a stateful packet filtering firewall. A stateful packet filtering firewall controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connectionless IP packets against a set of rules specified by the firewall's administrator. The PIX Firewall is administered from a separate platform referred to as the NT Workstation. The firewall detects the occurrence of selected events, gathers information concerning them, and sends that information to the NT Workstation where it is stored. The NT Workstation also detects the occurrence of selected events (e.g., security administrator actions), gathers information concerning them, and records it. Audit records can then be sorted and reviewed.

It is assumed that the TOE is located within a controlled access facility that mitigates unauthorized physical access and that the TOE is used only for firewall functionality. The TOE administrator is the only person allowed access to the TOE; there are no non-administrative accounts on the TOE. The administrator is assumed to be trustworthy and trained on security policies and practices of the environment for which the TOE is intended to protect. The TOE is intended to be used in environments in which either, at most, sensitive but unclassified information is processed or the sensitivity level of the information in both the internal and external networks is equivalent.

The evaluation was carried out in accordance to the TTAP process and scheme described in *Proposed TTAP Process for Common Criteria EAL 1&2 Evaluations* and *TTAP Scheme*. The purpose of the evaluation was to demonstrate that the TOE meets the security requirements contained in the Security Target. The criteria against which the TOE was judged are described in the *Common Criteria for Information Technology Security Evaluation*. Four certifiers on behalf of the TTAP Oversight Board monitored the evaluation carried out by Computer Sciences Corporation. The evaluation was completed in December 1998.

Computer Sciences Corporation has determined that the Security Target is conformant to the *U.S. Government Traffic-Filter Firewall Protection Profile for Low Risk Environments*. Computer Sciences Corporation has determined that the evaluation assurance level (EAL) for the product, as specified in the Security Target, is EAL2 and the product satisfies all the security functional requirements stated in the Security Target.

## 1.0 Introduction

This document describes the results of Trust Technology Assessment Program (TTAP) evaluation of the security protection provided by the Cisco PIX Firewall 520 Version 4.3(1) configured as described in the *Cisco PIX Firewall 520 Version 4.3(1) Installation and Configuration White Paper*. This product was examined by Computer Sciences Corporation in cooperation with Cisco Systems personnel. The security features of the Cisco PIX Firewall were examined against the requirements specified in the *Cisco PIX Firewall 520 Version 4.3(1) Security Target* in order to establish a candidate rating.

The evaluation was carried out in accordance with the TTAP process and scheme described in the *Proposed TTAP Process for Common Criteria EAL 1&2 Evaluations and TTAP Scheme*. The purpose of the evaluation was to demonstrate that the TOE meets the security requirements contained in the Security Target. The criteria against which the TOE was judged are described in the *Common Criteria for Information Technology Security Evaluation*. The evaluation was completed in December 1998.

Computer Sciences Corporation has determined that the Security Target is conformant to the *U.S. Government Traffic-Filter Firewall Protection Profile for Low Risk Environments*. Computer Sciences Corporation has determined that the evaluation assurance level (EAL) for the product, as specified in the Security Target, is EAL2 and the product satisfies all the security functional requirements stated in the Security Target.

### 1.1 Background

The TTAP is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called TTAP Evaluation Facilities (TEFs) using the current NSA evaluation methodology and proposed evaluation methodology for Evaluation Assurance Level (EAL)1 and EAL2 in accordance with cooperative research and development agreements. The program focuses on products with features and assurances characterized by the Trusted Computer System Evaluation Criteria (TCSEC) C2 and B1 level of trust and the Common Criteria (CC) EAL1 through EAL4.

The TTAP Oversight Board monitors the TEFs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a TEF and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is to be added to NSA's Evaluated Products List.

### 1.2 Document Organization

This document consists of ten chapters and several supporting appendices. Chapter 1 introduces the report. Chapter 2 identifies the Target of Evaluation (TOE) and provides an architectural overview of the TOE. Chapter 3 describes the TOE's security policy. Chapter 4 describes the security aspects of the environment and configuration in which

the TOE is expected to be used. Chapter 5 lists the product documentation provided to the consumer by the vendor. Chapter 6 describes both the developer and evaluator testing efforts. Chapter 7 presents the evaluation team's approach to performing the evaluation and their findings and conclusions. Chapter 8 provides evaluator comments and recommendations about the product. Chapter 9 is the glossary, and Chapter 10 lists all referenced documentation used as source materials while compiling this report or conducting the evaluation.

The supporting appendices provide the TOE Security Target; and a snapshot of the configuration parameters and files used during evaluator tests.

## 2.0 Identification

The Cisco PIX Firewall 520 Version 4.3(1), referred to as the Target of Evaluation (TOE), consists of the hardware and software components described in Table 1.

**Table 1 TOE Identification**

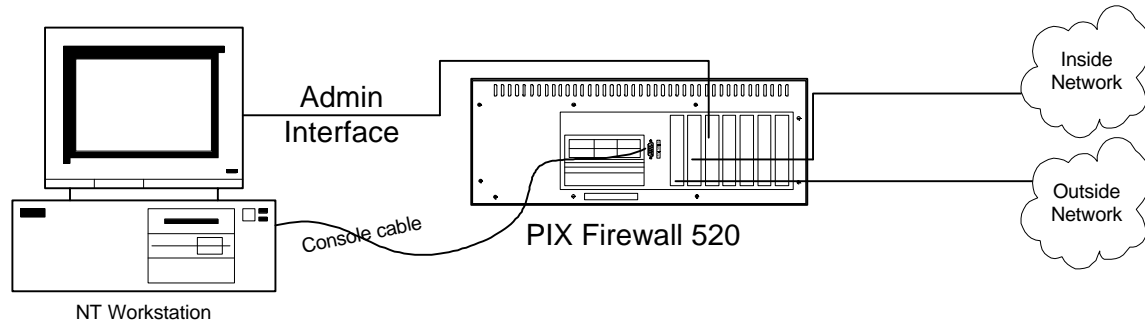
Platform	Component
PIX Firewall	<u>Hardware:</u> PIX 520 with Finesse V3.3 embedded operating system
	<u>Software:</u> PIX Firewall Version 4.3(1)
NT Workstation	<u>Hardware:</u> Intel Pentium II 333MHz PC with 64+MB of RAM, 6GB of hard disk, 3.5 floppy drive, tape drive, keyboard, mouse, serial port, color monitor, power cord, and 10/100Mbps Ethernet Network Interface Card with Windows NT 4.0 device driver
	<u>Software:</u> Windows NT 4.0 Workstation with Service Pack 3; PIX Firewall Syslog Server 4.3.1; TACACS+ Version 1.0; Microsoft Access 7.0; pfssfmt 1.0; and logfmt 1.0.

### 2.1 Evaluated Configuration

The evaluated configuration of the TOE consists of:

- ◆ One PIX Firewall, which controls the flow of IP traffic between the network elements; and
- ◆ One NT Workstation, by means of which administrators manage the security of the PIX Firewall.

The PIX Firewall provides three network interfaces; one of which is dedicated to NT Workstation. The dedicated interface is protected by the PIX Firewall, and no user traffic is allowed onto this network link. In addition, the console port on the PIX Firewall is used to allow system administration from the NT Workstation. Figure 1 illustrates this evaluated configuration. Syslog on the PIX Firewall is enabled to facilitate troubleshooting. By default, all internal (protected) and external (unprotected) hosts are blocked from initiating connections or sessions. Appendix B presents the configuration file and parameter settings for the default and testing configurations that were used for the evaluation.



**Figure 1 Evaluated Configuration**

The evaluation was limited to the software components that make up the TOE Security Functions (TSF) interfaces and TSF architecture in satisfaction of the functional requirements specified the *Cisco PIX Firewall 520 Version 4.3(1) Security Target*. Software and hardware features outside the scope of the defined TSF and thus not evaluated are:

- ◆ Cut-Through Proxies
- ◆ Failover
- ◆ PIX Firewall Manager
- ◆ Java and URL Filtering
- ◆ Mail Guard
- ◆ Network Address Translation (NAT)
- ◆ Private-Link
- ◆ Setup Wizard
- ◆ TFTP Configuration Server
- ◆ Virtual Private Networks (Ravlin IPsec Encryption Card)
- ◆ Remote Administration (Telnet interface)
- ◆ Acceptance of updates for internal data structures (e.g., routing tables) from an authorized host
- ◆ Windows NT 4.0 features not used by the TOE

The software and hardware features outside the scope of the evaluation are not enabled or used by the TOE. If these features are enabled then no statement regarding the satisfaction of security requirements can be made or assumed.

## **2.2 System Overview**

The TOE forms the boundary between an internal protected network and an external unprotected network. The TOE is physically protected such that TOE is located within controlled access facilities that mitigate unauthorized, physical access. All traffic

between the internal and external networks must flow through the TOE to maintain security. The external network may be accessible to the Internet and may contain systems that provide services such as HTTP, FTP, SMTP (electronic mail), and Telnet.

The TOE selectively routes information among internal and external networks according to rules established by an authorized administrator. The authorized administrator administers the PIX Firewall from the NT Workstation. Remote administration (telnet from the external or internal networks) to the TOE is prohibited in the evaluated configuration. The default configuration of the TOE prohibits all connections between networks. After the authorized administrator has configured information flow rules, the TOE limits connections between networks to only those which are authorized. The security features provided by the TOE include the following:

- ◆ Adaptive Security Algorithm – implements stateful connection control through the firewall.
- ◆ Access Lists – *outbound* and *apply* commands are used to control which internal systems can establish connections to the external network. By default, whichever hosts can initiate outbound connections can use all services during the outbound connection. The authorized administrator is able to restrict outbound connections in the following ways:
  - Deny or permit access to certain services
  - Restrict or permit access from an inside address or access to an outside address
- ◆ Conduits – *conduit* and *static* commands allow connections from the outside network to the inside network. The authorized administrator uses the *static* command to specify which IP addresses are visible on the outside interfaces for users to access and uses the *conduit* command to specify which services users can access on the internal hosts.
- ◆ System Log Messages – error and informational audit records are captured and stored for review by the authorized administrator. Audit records are stored on the NT Workstation in two separate types of files: event log and syslog files.
- ◆ Security Administration – a console interface is provided to allow restricted security administrative functions and interface. The authorized administrator administers the TOE from the NT Workstation. Security administrative functions are implemented on the PIX Firewall and the NT Workstation.
- ◆ Identification and Authentication – all users (i.e., authorized administrators) must identify and authenticate themselves before performing any security relevant action. The users are required to log into the NT Workstation and the PIX Firewall.

### 2.3 Hardware Overview

As shown in Figure 1, the TOE is composed of two physical platforms: the PIX 520, an Intel Pentium II-based computer; and the NT Workstation, an Intel Pentium II-based computer. The devices are connected by a Category 5 Crossover Network Ethernet cable shared with neither the external nor the internal networks. No user traffic is allowed onto this network link, and it is protected by the PIX Firewall. This link is primarily used by the PIX Firewall to forward syslog messages to the NT Workstation. The NT Workstation does not access resources on the external or internal networks. In addition, a DB9 to DB9 console cable provides the console interface for the authorized administrator to administer the PIX 520 from the NT Workstation.

The PIX 520 contains three 10/100 BaseT interface cards which provides the physical interfaces to the NT Workstation, the internal network, and the external network. The Motherboard on the PIX520 provides the interface for the console port and the floppy disk device. The floppy disk interface is used to initially load the PIX image and to back up configuration files. The flash ROM is an electrically erasable memory that holds the PIX software and configuration file. Specifically, the Flash provides the boot loader, PIX run time image, and the configuration file with access list rules.

The NT Workstation contains one 10/100Mbps Ethernet Network Interface Card (NIC) to provide the physical interface to the PIX 520. The tape drive is used to back up and recover user attributes and audit trail.

### 2.4 Software Overview

The TOE consists of the following software components that are security relevant and evaluated to satisfy the functional security requirements specified in the *Cisco PIX Firewall Version 4.3(1) Security Target*:

<u>Platform</u>	<u>Component</u>
PIX Firewall	PIX
	Network
	Command Interface
	Authentication/Authorization
	Finesse
	Syslog
	PC-BIOS
	PIX-BIOS
NT Workstation	TACACS+ Server

## PIX Firewall Syslog Server

## Conversion Tools

Windows NT (Event Log, Registry, NT TCP/IP stack, NT Security Subsystem, User Manager, NT File System)

Microsoft Access

### 2.4.1 PIX Firewall Software Components

The *PIX component* contains the Adaptive Security mechanism responsible for implementing the Adaptive Security Algorithm stateful packet filtering engine, and session proxy.

The *Network component* is responsible for all operations related to the handling of network traffic between the inside and outside network interfaces and network services.

The *Command Interface component* supports the command line interface used by the console. The Command Interface is also responsible for interpreting the PIX configuration commands from the terminal, memory, or floppy.

The *Authentication/Authorization component* implements the authentication challenge and response requests between the users (authorized administrator) and the *TACACS+ Server* executing on the NT Workstation.

The Cisco proprietary *Finesse* operating system provides the PIX Firewall threads with a device interface, cooperative Light Weight Process Scheduling, IP packet buffer management and temporary resource allocation and reallocation. Hardware device drivers, low level operating system functions, and system scheduling are provided by the proprietary *Finesse* software kernel. The *Finesse* also creates and manages the internal block structures associated with packets.

The *Syslog component* creates logging messages and routes them to the *PIX Firewall Syslog Server* executing on the NT Workstation using a TCP connection.

The *PC-BIOS* and *PIX-BIOS* together provide the startup sequence on the PIX Firewall. The *PC-BIOS* provides initial device startup and initialization and interrupt handling until the PIX boot loader can be executed. Once the boot loader is operational, the *PC-BIOS* is not executed, called, or accessed again.

The *PIX-BIOS* provides the PIX boot loader. The boot loader is responsible for completing the operating system loading and executing the stored configuration. When system loading is complete, the *PIX-BIOS* passes control to the *Finesse* operating system.

## 2.4.2 NT Workstation Software Components

When the administrator is prompted to login to the PIX Firewall, the PIX Firewall uses the *TACACS+ Server* on the NT Workstation to perform the authentication. The server uses the NT Registry to authenticate the authorized administrators trying to logon to the PIX Firewall. Audit records generated by the TACACS+ server are sent to Windows NT event log.

The *PIX Firewall Syslog Server* is a daemon process that collects syslog messages from the PIX Firewall. It writes to one of seven log files depending on the day of the week. In addition, the server generates its own audit messages and writes them to a separate syslog log file. The server is responsible for monitoring the disk space and, if approaching the preset threshold, will close the TCP connection to the PIX Firewall to control audit record generation and potential loss of audit information. The conversion tools, *pfssfmt* and *logfmt*, are used to convert the syslog files for import to a *Microsoft Access* database.

The TOE uses the *NT File System*, *Event Log*, *NT Security Subsystem*, *NT TCP/IP Stack*, *NT Security Subsystem*, and *User Manager* of the *Windows NT operating system*. The TOE uses these components to generate audit records, provide a search and sorting tool for audit records, perform identification and authentication of the authorized administrator, allow the NT Workstation and PIX Firewall to communicate, and allow the authorized administrator to configure the authentication policy.

*Microsoft Access* is used to search and sort on the audit information converted by and generated by the *pfssfmt* and *logfmt* utilities.

### 3.0 Security Policy

The PIX Firewall in the evaluation configuration helps prevent unauthorized connections between two networks. Connections between the networks are controlled by the firewall because all traffic between the networks must flow through the PIX firewall to maintain security. The PIX firewall enforces filtering rules established by an authorized administrator for controlling access to the networks.

The security policy enforced by the TOE Security Functions (TSF) addresses four areas: information flow control, identification and authentication, audit, and security administration.

The basic objective of the information flow control policy is to only allow services originating from either the internal or the external networks through the firewall if the firewall was configured to allow such access. The PIX Firewall's Adaptive Security Algorithm (ASA) mechanism is used to implement the information flow control security policy. The ASA mechanism allows a stateful packet filtering approach. Every inbound packet is checked against the ASA and against connection state information in memory. Relationships and rules are based on interface pairs. Each interface is assigned a security level in the range 0-100 where 100 is the most secure and 0 is the least secure. Interfaces with the same security level cannot communicate. The interface of the protected network (internal) is assigned a security level of 100; the interface of the unprotected network (external) is assigned a security level less than 100. The ASA mechanism controls the establishment of connections from one network to another as identified by the security levels between interfaces. The ASA mechanism follows these ASA security interface rules:

- ◆ No packets can traverse the PIX Firewall without a connection/state.
- ◆ Outbound connections/states are allowed, except those specifically denied by outbound lists. An outbound connection/state is one where the originator/client is on a higher security interface/network than the receiver/server.
- ◆ Inbound connections/states are denied, except those specifically allowed by conduits. An inbound connection/state is one where the originator/client is on a lower or equal security interface/network than the receiver/server.
- ◆ All attempts to circumvent the previous rules are dropped and a message is sent to the Syslog component.

The inherent ASA basic rules for information flow are as follows:

- ◆ Allow any TCP connection that originates from the inside network.
- ◆ Permit TCP packets from the outside network that are return packets for an existing outgoing connection.
- ◆ Drop and log attempts to initiate TCP or UDP connections from the outside network to any IP address for an existing connection.

- ◆ Drop and log source routed IP packets from the outside network that is sent to any IP address for an existing connection.
- ◆ Silently drop ping requests to IP addresses for an existing dynamic connection.
- ◆ Answer, by the PIX Firewall, ping requests directed to static connections.
- ◆ Allow any UDP connection that originates from the inside network.
- ◆ Drop and log all other packets received on the outside interface.
- ◆ UDP connection objects are timed out based on a configurable scheduling frequency timer, started when the connection object is created.
- ◆ TCP connection objects are timed out based on a configurable millisecond clock timer, started when the connection object is created.
- ◆ Drops packets that arrive on the outside interface with a source IP address on the inside network.

After the authorized administrator creates the default TOE configuration as specified in the *Cisco PIX Firewall 520 Version 4.3(1) Installation and Configuration White Paper*, the PIX Firewall rejects all outbound connections from the internal network to the unprotected, external network and rejects any connections inbound from the external network. This default information flow policy can be modified by the authorized administrator using the *outbound*, *apply*, *conduit*, and *static* commands. All decisions on requests for information flow are audited.

The TOE supports one type of user, the authorized administrator. The authorized administrator is restricted to an administrator role to perform security administration of the TOE. The authorized administrator must identify and authenticate himself or herself to the TOE before performing any security relevant action. The security administration capabilities provided by the TOE include setting information flow security policies; assigning users to the authorized administrator role; modifying the time and date; managing the audit trail; and backup and recovery. Management of the audit trail and user accounts is audited.

## **4.0 Assumptions and Clarification of Scope**

The TOE is intended to be used in environments in which either, at most, sensitive but unclassified information is processed, or the sensitivity level of the information in both the internal and external networks is equivalent.

### **4.1 Usage Assumptions**

The assumptions made about the usage of the TOE are identified in Section 3.1, Assumptions, of the *Cisco PIX Firewall 520 Version 4.3(1) Security Target*.

### **4.2 Environmental Assumptions**

The assumptions about the environment for which the TOE is to be used are identified in Section 3.1, Assumptions, of the *Cisco PIX Firewall 520 Version 4.3(1) Security Target*.

### **4.3 Clarification of Scope**

The threats addressed by the TOE and for which specific protection within the TOE or its environment is required are described in Section 3.2, Threats, in the *Cisco PIX Firewall 520 Version 4.3(1) Security Target*. The IT security requirements of the TOE are traceable to security objectives derived from the assumptions and threats identified in Section 3.0, TOE Security Environment, of the *Cisco PIX Firewall 520 Version 4.3(1) Security Target*. Threats that are not listed in Section 3.2 are not recognized as being addressed by the TOE because the IT security requirements for which the TOE was evaluated were not derived to counter these threats. Thus, no assumptions or claims can be made about the ability of the TOE to counter threats not specified in Section 3.2.

## 5.0 Documentation

The vendor provides the following product documentation to the consumer:

- Cisco PIX Firewall 520 Version 4.3(1) Administrative Guidance White Paper, Version 1.0  
TTAP document describing how to administer the TOE. This document includes a description of all audit record events.
- Cisco PIX Firewall 520 Version 4.3(1) Installation and Configuration White Paper Version 1.0  
TTAP document describing how to install and configure the TOE. The resulting default configuration prescribed by this document denies all flows (incoming and outgoing) through the box.
- Cisco PIX Firewall 520 Version 4.3(1) Security Target Version 1.2  
TTAP evaluation document describing Cisco's security functionality and compliance to the U.S. Government Traffic-Filter Protection Profile for Low Risk Environments.
- Configuration Guide for the PIX 4.2  
Standard Cisco documentation for the PIX Firewall.
- Release Notes for the PIX Firewall 4.2  
Standard Cisco documentation for the PIX Firewall.
- PIX Firewall Quick Installation Guide 4.2  
Standard Cisco documentation for the PIX Firewall.
- System Log Messages for the PIX Firewall, Version 4.2  
Standard Cisco documentation for the PIX Firewall.

## 6.0 Product Testing

This chapter describes the functional and penetration testing effort performed as part of the evaluation. This effort included the evaluation team's executing all the developer's test suites, according to the developer-provided test documentation, and executing the team's own tests. The developer's test addressed all the security functional requirements (SFRs) stated in the *Cisco PIX Firewall 520 Version 4.3(1) Security Target* except for areas concerning deny rule enforcement of loop back and broadcast source addresses, and audit management. The evaluator tests covered those areas not addressed by the developer tests. The evaluator tests primarily concentrated on the policy enforcement mechanism.

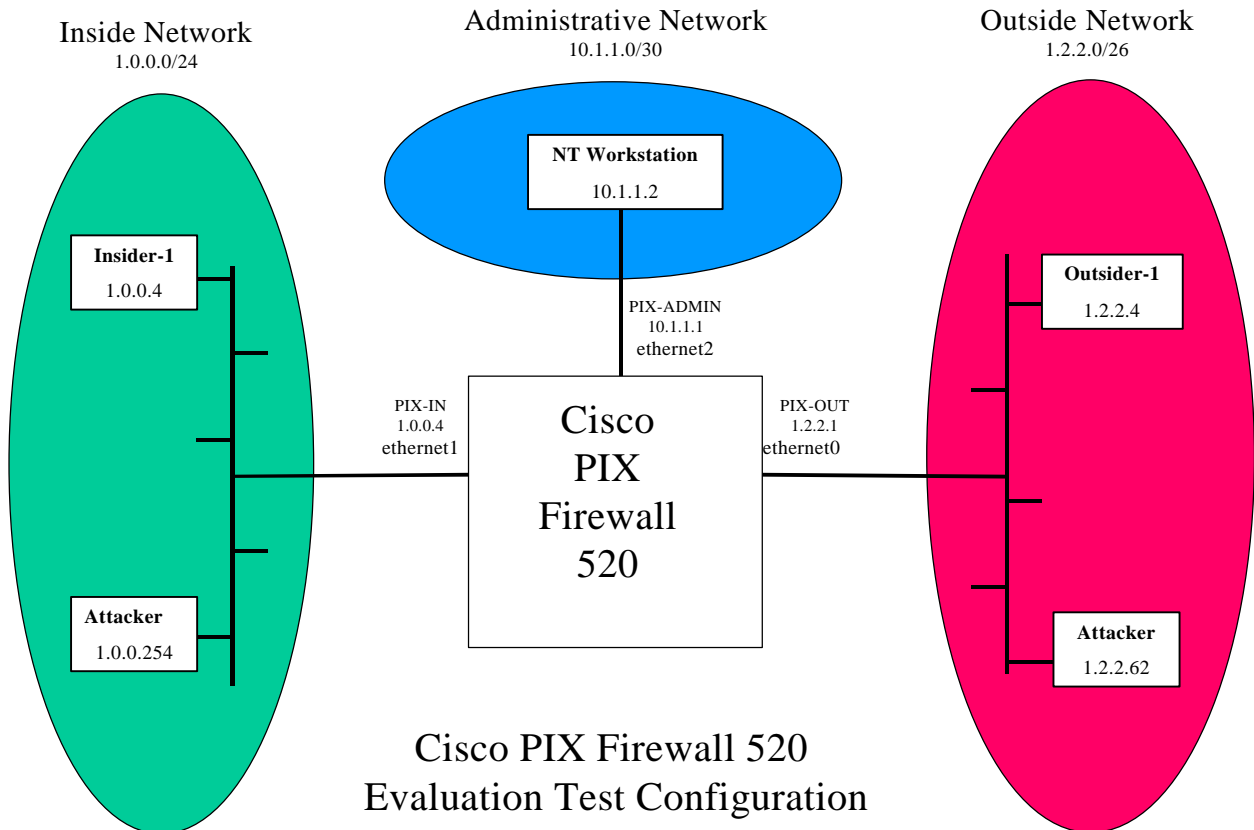
### 6.1 TOE Configurations Used in Testing

Table 2 identifies the TOE hardware and software components used by the evaluation team during testing.

**Table 2 TOE Components for Testing**

Platform	Component
PIX Firewall	<u>Hardware:</u> PIX 520 with Finesse V3.3 embedded operating system
	<u>Software:</u> PIX Firewall Version 4.3(1) image
NT Workstation	<u>Hardware:</u> Intel Pentium II 333MHz PC with 64 MB of RAM, 6GB of hard disk, 3.5 floppy drive, tape drive, keyboard, mouse, serial port, color monitor, power cord, and 10/100mbps Ethernet Network Interface Card with Windows NT 4.0 device driver
	<u>Software:</u> Windows NT 4.0 Workstation with Service Pack 3; PIX Firewall Syslog Server 4.3.1; TACACS+ Version 1.0; Microsoft Access 7.0; pfssfmt 1.0; and logfmt 1.0

The test bed configuration is described in Figure 2. It consisted of internal, external, and administrative network segments. The internal and external segments were composed of one or more end-system computers, a network monitor, and a test generator, connected via a non-switching hub. The administrative network was composed of the administrative workstation and a network monitor.



**Figure 2 TOE Test Configuration**

The TOE was configured as directed in the *Cisco PIX Firewall 520 Version 4.3(1) Installation and Configuration White Paper*, yielding the default TOE configuration file described in Appendix B.

Subsequent to testing of the default configuration, the PIX Firewall component was configured, using the *Outbound* and *Apply* commands, to permit connections from the inside network to the outside network. Then, *Outbound-Only* testing was performed to demonstrate that the PIX permitted only connections from the inside network to the outside network in conformance with the new rules, while prohibiting flow from the outside network to the inside network. Appendix B presents an example configuration rule set used for *Outbound-Only* testing.

Last, after testing the *Outbound-Only* configuration, the PIX Firewall component was configured, using the *Static* and *Conduit* commands, to permit connections from the outside network to the inside network. Then, *Two-Way* testing was performed to demonstrate that the PIX permitted only connections from the inside network to the outside network or from the outside network to the inside network permitted by the rules. Appendix B presents an example configuration rule set used for *Two-Way* testing.

The evaluation team used the following utilities to conduct functional and penetration tests:

- CSC Hydra <sup>TM</sup> Tool Kit
- Cisco NetSonar
- Microsoft Network Monitor

## **6.2 Results of Developer Testing**

The vendor's tests were grouped by security functional areas, which mapped to the security functions defined in the *Cisco PIX Firewall 520 Version 4.3(1) Security Target*. The evaluation team executed all the developer's test scenarios. The majority of the tests executed as described in the developer's test documentation. Initially, tests for information flow control and audit requirements did not execute as described. However, the developer addressed most of these anomalies through changes to the PIX firewall image. The remaining were fixed through modifications to the default configuration with accompanying guidance to administrators.

## **6.3 Results of Evaluator Testing**

The evaluation team performed two classes of test:

- Functional tests to cover those security requirements not addressed by the developer tests.
- Penetration tests concentrated on the policy enforcement mechanism of the TOE.

Functional tests included:

- Validation of the procedures described in *Cisco PIX Firewall 520 Version 4.3(1) Installation and Configuration White Paper*.
- Validation of the commands described in *Cisco PIX Firewall 520 version 4.3(1) Administrative Guidance White Paper*.
- Correctness of the mechanisms enforcing the information flow rules established by the administrator.

Penetration tests were based on the developer's vulnerability assessment, attacks available in the public domain, and vulnerabilities derived from evaluator observations during functional testing. Penetration tests included:

- Attacks identified in Appendix A of the *U.S. Government Traffic-Filter Firewall Protection Profile for Low Risk Environments* appropriate given the architecture of the TOE;
- Exploitation of ports 23 and 1467 being "active" on "inside" interface of PIX;
- Exploitation of sequence numbers on inside interface not changing after half-open connection;

- Exploitation of port 9999 on "outside" interface of PIX responding to connect from "inside";
- Passing of final fragment of fragmented SYN packet passes "inside" to "outside";
- Exploitation of broadcast source address;
- Exploitation of loopback source address;
- Exploitation of packets with "spoofed" source addresses;
- "Tailgating" packets for same "connection" passed through PIX;
- Exploitation of fragmented packet passes outside to inside with conduit disabled; and
- Zero length UDP packet to port 520

Initially, anomalies were identified. The developer addressed most of these through changes to the PIX firewall image. The remainder was addressed through changes to the default configuration with accompanying administrator guidance.

## 7.0 Results of the TOE Evaluation

This chapter documents the functional and assurance requirements that the product satisfies and how the evaluation team verified the requirements satisfaction. A description of these requirements and details of how the product meets each of them can be found in the *U.S. Government Traffic-Filter Firewall Protection Profile for Low Risk Environments* and the *Cisco PIX Firewall Version 4.3(1) Security Target*, respectively.<sup>1</sup>

### 7.1 TOE Security Requirements

The security functional requirements (SFRs) of the TOE consist of the following Common Criteria functional components summarized in Table 3. These requirements were derived from the *U.S. Government Traffic-Filter Firewall Protection Profile for Low Risk Environments* (referred to as the TFFPP). The following TFFPP requirement components were omitted because the evaluated TOE configuration was configured not to include remote administration to the TOE and updates of the TOE information by authorized external IT entities: FIA\_AFL.1, FIA\_UAU.4, and FCS\_COP.1.

**Table 3 TOE Functional Requirements**

Functional Components	
FMT_SMR.1	Security Roles
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action
FIA_UAU.1	Timing of authentication
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FMT_MSA.3	Static attribute initialization
FDP_RIP.2	Full residual information protection
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time and date stamps
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review

<sup>1</sup> TFFPP Version 1.c was the final version used for this evaluation.

Functional Components	
FAU_STG.1	Protected audit trail storage
FAU.STG.4	Prevention of audit data loss
FMT_MOF.1	Management of security functions behavior

The assurance requirements of the TOE consist of the requirements for EAL2 defined in Part 3 of the Common Criteria summarized in Table 4.<sup>2</sup>

**Table 4 TOE Assurance Requirements**

Assurance Class	Assurance Components	
Configuration management	ACM_CAP.2	Configuration items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

## 7.2 Evaluation Approach

The evaluation team's approach to evaluating the TOE was mandated by Part 3 of the Common Criteria, Section 2.1.3.5:

"Evaluator actions, combined with the requirements of content and presentation of evidence, identify the evaluator effort that shall be expended in verifying the security claims made in the ST of the TOE."

The evaluation was conducted by following the evaluator actions elements defined by the EAL2 requirements using an evaluated Security Target (ST) as the basis<sup>3</sup>. To manage the

<sup>2</sup> The AGD\_USR.1 requirements were not applicable for this evaluation because the TOE does not have users for which a user's guide is needed. The only human user accessing the TOE is the authorized administrator and guidance for the administrator is presented in the administrator guide covered by AGD\_ADM.1

<sup>3</sup> CSC conducted an informal evaluation of the ST against the ASE requirements presented in Part 3 of the Common Criteria. Although a working draft, the ST was deemed by CSC to be in a reasonable state to allow the evaluation to proceed. NSA is responsible for formally evaluating the ST.

evaluation effort and to document progress and findings, the evaluation team developed an evaluation work package report for each assurance family. A work package captures every evaluator action element for the assurance family and allows the evaluator to document how each action element is addressed during the evaluation. The work packages were also used to formally document comments concerning evaluation evidence and were submitted to the vendor. For the development and testing assurance families, the evaluation team used the Derived Testing Requirements for the TFFPP as a reference to examine the satisfaction of security functional requirements.<sup>4</sup>

Throughout the evaluation, the evaluation team generated Observation Reports (ORs) to request clarification on TFFPP or Common Criteria requirements. Some of the ORs did result in changes to the TFFPP.<sup>5</sup>

### **7.3 Requirement Verification**

This section presents how the evaluation team confirmed that the TOE meets the security requirements summarized in Table 3 and Table 4 by describing the evaluation effort performed for each EAL2 assurance family.

#### **7.3.1 Configuration Management**

##### **ACM\_CAP.2 Configuration items**

Requirement Verification. The evaluation team confirmed the content and presentation of evidence requirements of ACM\_CAP.2 by inspection of the vendor-supplied *Configuration Management and Delivery Procedures* document.

Verdict. The TOE passes the ACM\_CAP.2 requirements.

#### **7.3.2 Delivery and Operation**

##### **ADO\_DEL.1 Delivery procedures**

Requirement Verification. The evaluation team confirmed the content and presentation of evidence requirements of ADO\_DEL.1 by inspection of the vendor-supplied *Configuration Management and Delivery Procedures* document.

Verdict. The TOE passes the ADO\_DEL.1 requirements.

##### **ADO\_IGS.1 Installation, generation, and start-up procedures**

---

<sup>4</sup> Specifically, the evaluation team referenced the *Common Criteria Testing Program Derived Test Requirements of the U.S. Government Traffic Filter Firewall Protection Profile for Low Risk Environments*.

<sup>5</sup> Two versions of the TFFPP were used during the evaluation. Version 1.a was used initially with ORs generated against it. Version 1.c was later generated to address those ORs. Upon completion of the evaluation, Version 1.c was the most current version of the TFFPP used by the evaluation team.

Requirement Verification. The evaluation team confirmed the content and presentation of evidence requirements of ADO\_IGS.1 by inspection of the vendor-supplied *Cisco PIX Firewall 520 Version 4.3(1) Installation and Configuration White Paper* document. In addition, the team determined that the installation, generation, and start-up procedures resulted in a secure configuration by following the installation and generation instructions as part of functional testing.

Verdict. The TOE passes the ADO\_IGS.1 requirements.

### 7.3.3 Development

#### ADV\_FSP.1 Informal functional specification

Requirement Verification. The functional specification provided by the developer encompassed the following documents:

- *Cisco PIX Firewall 520 Version 4.3(1) Security Target*, Version 1.2
- *Cisco PIX Firewall 520 Version 4.3(1) Administrative Guidance White Paper*, Version 1.0
- *System Log Messages for the PIX Firewall*, Version 4.2
- *Configuration Guide for the PIX 4.2*
- *PIX Firewall Quick Installation Guide 4.2*
- *Hardware Functional Specification (Lego)*, Revision 1.2

The evaluation team confirmed the content and presentation of evidence requirements of ADV\_FSP.1 by inspection of the above-mentioned documents. The TOE Summary Specification of the Security Target was examined by the evaluation team to determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

Verdict. The TOE passes the ADV\_FSP.1 requirements.

#### ADV\_HLD.1 Descriptive high-level design

Requirement Verification. The High-Level Design provided by the developer encompassed the following documents:

- *NT Workstation Architecture Document*, Version 1.0
- *PIX Firewall Syslog Server White Paper*, Version 2.3
- *PIX V4.3.1 Architecture and Detailed Design*, Version 1.2

The evaluation team confirmed the content and presentation of evidence requirements of ADV\_HLD.1 by inspection of the above-listed documents. The documents were examined by the evaluation team to determine that the High-

Level Design is an accurate and complete instantiation of the TOE security functional requirements.

Verdict. The TOE passes the ADV\_HLD.1 requirements.

### **ADV\_RCR.1 Informal correspondence demonstration**

Requirement Verification. The evaluation team confirmed the content and presentation of evidence requirements of ADV\_RCR.1 by inspection of the vendor-supplied *Cisco PIX Firewall 520 Version 4.3(1) Correspondence White Paper*, Version 1.0 document.

Verdict. The TOE passes the ADV\_RCR.1 requirements.

## **7.3.4 Guidance Documents**

### **AGD\_ADM.1 Administrator guidance**

Requirement Verification. The evaluation team confirmed the content and presentation of evidence requirements of AGD\_ADM.1 by inspection of the vendor-supplied *Cisco PIX Firewall 520 Version 4.3(1) Administrative Guidance White Paper*, Version 1.0 document and the *Cisco PIX Firewall 520 Version 4.3(1) Installation and Configuration White Paper* document. The guidance was verified as part of functional testing.

Verdict. The TOE passes the AGD\_ADM.1 requirements.

### **AGD\_USR.1 User guidance**

Requirement Verification. Since the TOE security environment assumes that non-administrator users do not have access to the TOE and the TOE does not provide functionality to allow authorized external IT entities to access the TOE, this requirement is not applicable. The evaluation team did confirm through testing that the TOE denies unauthorized access to the TOE.

## **7.3.5 Tests**

### **ATE\_COV.1 Evidence of coverage**

Requirement Verification. The evaluation team confirmed the content and presentation of evidence requirements of ATE\_COV.1 by inspection of the vendor supplied *Cisco PIX Target of Evaluation Test Procedures Document*, Version 1.0 document.

Verdict. The TOE passes the ATE\_COV.1 requirements.

## ATE\_FUN.1 Functional testing

Requirement Verification. The evaluation team confirmed the content and presentation of evidence requirements of ATE\_FUN.1 by inspection of the vendor supplied *Cisco PIX Target of Evaluation Test Procedures Document*, Version 1.0 document.

Verdict. The TOE passes the ATE\_FUN.1 requirements.

## ATE\_IND.2 Independent testing – sample

Requirement Verification. The evaluation team confirmed the content and presentation of evidence requirements of ATE\_IND.2 by creating a test environment that allowed the TOE to be suitable for testing. All the developer tests as documented in *Cisco PIX Target of Evaluation Test Procedures Document*, Version 1.0 were executed by the evaluation team and verified against the developers test results. To test a subset of the TSF, the evaluation team performed additional functional and penetration tests in the areas of rule enforcement and TSF architecture and confirmed the TOE operates as specified.

Table 5 identifies test coverage of each SFR. Tests denoted as tested by the developer were re-executed by the evaluation team. Tests denoted as tested by the evaluator means new tests were created and executed by the evaluation team.

**Table 5 Test Coverage of Security Functional Requirements**

SFR	Tested by
FMT_SMR.1	Developer
FIA_ATD.1	Developer
FIA_UID.2	Developer
FIA_UAU.1	Developer
FDP_IFC.1	Developer; Evaluator (as part of penetration tests)
FDP_IFF.1	Developer (except FDP_IFF1.6(c)(d)); Evaluator (as part of penetration tests)
FMT_MSA.3	Developer; Evaluator
FDP_RIP.2	Evaluator (as part of penetration tests)
FPT_RVM.1	Evaluator (as part of penetration tests)
FPT_SEP.1	Developer; Evaluator (as part of penetration tests)

SFR	Tested by
FPT_STM.1	Developer
FAU.GEN.1	Developer; Evaluator
FAU.SAR.1	Developer
FAU.SAR.3	Developer
FAU_STG.1	Developer
FAU.STG.4	Evaluator
FMT_MOF.1	Developer (except audit capabilities); Evaluator (only audit, backup, and recovery capabilities)

Problems found during evaluator testing were reported to the vendor. The TOE was regression tested to verify the identified problems were fixed.

Verdict. The TOE passes the ATE\_IND.2 requirements.

### 7.3.6 Vulnerability Assessment

#### AVA\_SOF.1 Strength of TOE security function evaluation

Requirement Verification. The evaluation team confirmed the content and presentation of evidence requirements of AVA\_SOF.1 by inspection of the strength of function claim supplied in Appendix A of the *Cisco PIX Firewall 520 Version 4.3(1) Administrative Guidance White Paper*, Version 1.0 document. The evaluation team confirmed that the claim was correct by examining the mathematics.

Verdict. The TOE passes the AVA\_SOF.1 requirements.

#### AVA\_VLA.1 Developer vulnerability analysis

Requirement Verification. The evaluation team confirmed the content and presentation of evidence requirements of AVA\_VLA.1 by inspection of the vendor-supplied *TTAP PIX Firewall Vulnerability Assessment*, Version 1.0 document. The evaluation team confirmed the developer's vulnerability analysis results by conducting penetration tests that searched for obvious vulnerabilities as defined in the TFFPP Appendix A, and presented in the *TTAP PIX Firewall Vulnerability Assessment* document. In addition, the evaluation team did perform an independent search for obvious vulnerabilities building on those reported in the public domain. Discovered vulnerabilities were reported to the developer. The evaluation team regression tested the TOE and confirmed that no obvious

vulnerabilities were exploitable in the intended environment for the TOE in its evaluated configuration.

Verdict. The TOE passes the AVA\_VLA.1 requirements.

#### **7.4 Functional Requirement Satisfaction**

This section describes how the TOE meets the SFRs specified in the *Cisco PIX Firewall 520 Version 4.3(1) Security Target*. The evaluation team confirmed that these requirements are satisfied by the TOE by examining the design and behavior descriptions presented in the Functional Specification, High-Level Design, Administrator Guide, and Test Documentation and through functional and vulnerability testing.

##### **7.4.1 FMT\_SMR.1 Security roles**

###### Requirement.

FMT\_SMR.1.1 - The TSF shall maintain the role authorized administrator.

FMT\_SMR.1.2 - The TSF shall be able to associate human users with the authorized administrator role.

###### Applicable Features.

The TOE relies on the NT Workstation to maintain the authorized administrator role by using group assignment. The “administrator” group is used on the NT Workstation to define the administrator role. The Security Target assumes that the TOE environment only allows authorized administrators to access the TOE. There are no non-administrator accounts on the TOE. When a user logs into the NT Workstation, they are automatically assigned to the administrator role because their user account is defined to include the ‘administrator’ group.

Conclusion. The TOE satisfies the FMT\_SMR.1 requirements.

##### **7.4.2 FIA\_ATD.1 User attribute definition**

###### Requirement

FIA\_ATD.1.1 - The TSF shall maintain the following list of security attributes belonging to individual users:

- a) identity
- b) association of a human user with the authorized administrator role
- c) no additional user attributes

### Applicable Features

The NT Security Subsystem on the NT Workstation maintains the security attributes (unique identity and role assignment) for each user account. An identity is formed by a unique user name (defined by the administrator) and user id (generated by the NT Security Subsystem). Windows NT does not allow an existing user name to be reused and assigned to a separate account. When a user logs into the NT Workstation, they are automatically assigned to the administrator role because their user account is defined to include the 'administrator' group.

Conclusion. The TOE satisfies the FIA\_ATD.1 requirement.

## **7.4.3 FIA\_UID.2 User identification before any action**

### Requirement

FIA\_UID.2.1 - The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

### Applicable Features

The only human users having accounts on the NT Workstation are authorized administrators. They must first identify themselves using their assigned user name and supply a password before any TSF action takes place. External IT entities are identified by IP address and the PIX interface (inside, outside) that the IP address is identified on. This IP address is validated against the configuration rules before any flow is allowed through the TOE.

Conclusion. The TOE satisfies the FIA\_UID.2 requirement.

## **7.4.4 FIA\_UAU.1 Timing of authentication**

### Requirement

FIA\_UAU.1.1 - The TSF shall allow identification as stated in FIA\_UID.2 on behalf of the authorized administrator or authorized external IT entity accessing the TOE to be performed before the authorized administrator or authorized external IT entity is authenticated.

FIA\_UAU.1.2 - The TSF shall require each authorized administrator or authorized external IT entity to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that authorized administrator or authorized IT entity.

### Applicable Features

The TOE is not configured to support authorized external IT entities. For authorized administrators, a prompt for identity (user name) and password is displayed to the user

when the NT Workstation is started up or rebooted. The *Cisco PIX Firewall 520 Version 4.3(1) Administrative Guidance White Paper* recommends the password to be at least 8 symbols long, and at least one of which is a digit or special symbol. Once the user is successfully authenticated, the TOE will allow other TSF mediated actions to take place on behalf of the user. If the user is not successfully authenticated, the prompt for identity and password is redisplayed.

Conclusion. The TOE satisfies the FIA\_UAU.1 requirements.

#### **7.4.5 FDP\_IFC.1 Subset information flow control**

##### Requirement

FDP\_IFC.1.1 - The TSF shall enforce the UNAUTHENTICATED SFP on:

- a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another.
- b) information: traffic sent through the TOE from one subject to another.
- c) operation: pass information.

##### Applicable Features

The information flow policy enforced by the TOE is defined by the basic rule set of the PIX Firewall's ASA (presented in Section 3.0) and the information flow rules defined by the administrator. The ASA mechanism enforces these rules on a packet-by-packet basis.

Conclusion. The TOE satisfies the FDP\_IFC.1 requirement.

#### **7.4.6 FDP\_IFF.1 Simple security attributes**

##### Requirement

FDP\_IFF.1.1 - The TSF shall enforce the UNAUTHENTICATED SFP based on at least the following types of subject and information security attributes:

- a) subject security attributes
  - presumed address
  - no additional subject security attributes
- b) information security attributes

- presumed address of source subject
- presumed address of destination subject
- transport layer protocol
- TOE interface on which traffic arrives and departs
- service
- no additional information security attributes

FDP\_IFF.1.2 - The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold:

- a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:
  - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator.
  - the presumed address of the source subject, in the information, translates to an internal network address.
  - the presumed address of the destination subject, in the information, translates to an address on the other connected network.
- b) Subjects on the external network can cause information to flow through the TOE to another connected network if:
  - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator.
  - the presumed address of the source subject, in the information, translates to an external network address.
  - the presumed address of the destination subject, in the information, translates to an address on the other connected network.

FDP\_IFF.1.6 - The TSF shall explicitly deny an information flow based on the following rules:

- a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network.
- b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network.
- c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network.
- d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network.

### Applicable Features

The security attributes used by the ASA mechanism to enforce the information flow policy are as follows: the PIX firewall interface (on which the packet arrives), and its associated “security level”, IP layer source address, IP layer destination address, transport layer protocol (TCP, UDP, ICMP), and services identified by port numbers at the transport layer.

A deny or permit information flow rule is defined using these security attributes. The *outbound/apply* commands are used to permit access to external resources from internal hosts based on the defined security attributes (used in any combination). The *conduit/static* commands are used to permit limited access to internal resources from external hosts based on defined security attributes (used in any combination). The ASA basic rule set (presented in Section 3.0) includes a rule to drop packets that arrive on one interface with a source address of the destination network. It also drops all packets with a source address on the loopback (127.x.x.x ) network as well as packets containing source address with a known broadcast address.

Conclusion. The TOE satisfies the FDP\_IFF.1 requirements.

### **7.4.7 FMT\_MSA.3 Static attribute initialization**

#### Requirement

FMT\_MSA.3.1 - The TSF shall enforce the information flow control UNAUTHENTICATED SFP to provide restrictive default values for information flow security attributes that are used to enforce the SFP.

FMT\_MSA.3.2 - The TSF shall allow an authorized administrator to specify alternative initial values to override the default values when an object or information is created.

### Applicable Features

The TOE taken out of the box denies all traffic to flow through the PIX Firewall because a configuration file has not been installed. The basic rules of the ASA will allow all outbound connections and deny all inbound connections. At a minimum, once interfaces are defined and saved in the configuration file, the basic rules will take into effect unless there are explicit rules defined by the administrator that override the basic rules.

After completion of the installation, generation, and startup procedures in *Cisco PIX Firewall 520 Version 4.3(1) Installation and Configuration White Paper*, the TOE will deny all inbound and outbound traffic. It was considered under this evaluation that the default configuration for the TOE is established after completion of the installation, generation, and startup procedures. Thus, the TOE enforces the most restrictive information flow rules (deny all) for inbound and outbound flows in the default configuration. The administrator is able to override the default values by using the *outbound/apply* and *conduit/static* commands.

Conclusion. The TOE satisfies the FMT\_MSA.3 requirements.

## **7.4.8 FDP\_RIP.2 Full residual information protection**

### Requirement

FDP\_RIP.2.1 - The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to all subjects.

### Applicable Features

When a new packet is received by the PIX Firewall, the finesse operating system creates a block structure for the packet, overwriting any information contained in the memory area allocated for the block structure, and defines block pointers with size information for other internal components to access the block. When the packet is reconstructed, the block pointers are used to access the data that was originally written to the block. No residual information is obtained from a previously sent packet because the packet is reconstructed from the block data elements.

Conclusion. The TOE satisfies the FDP\_RIP.2 requirement.

## **7.4.9 FPT\_RVM.1 Non-bypassability of the TSP**

### Requirement

FPT\_RVM.1.1 - The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

### Applicable Features

All packets are received by a network interface card and translated into a block structure. Multiplexing, integrity checks, and block boundary markings are then performed on the received blocks before sending the block on to the ASA mechanism. The ASA basic information flow rules and configuration information flow rules are used by the ASA mechanism to determine if the flow should be allowed through the TOE. Failure to satisfy a flow rule causes a syslog message to be generated, the connection denied, and the packet is dropped. If the ASA mechanism determines that the block (packet) satisfies the flow rules, the block is processed (the packet reconstructed) and sent to its destination interface.

Conclusion. The TOE satisfies the FPT\_RVM.1 requirement.

#### **7.4.10 FPT\_SEP.1 TSF domain separation**

##### Requirement

FPT\_SEP.1.1 - The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT\_SEP.1.2 - The TSF shall enforce separation between the security domains of subjects in the TSC.

##### Applicable Features

The TOE is defined to have no untrusted subjects. Only firewall related applications are executing on the TOE. The TOE is assumed to be in a controlled area and only accessible by authorized administrators.

The TOE scope of control is defined as the following: connections between subjects mediated by the TSF such that each connection is a separate domain. Access through the TOE is only permitted based on security policy enforced by the PIX Firewall configuration defined by an authorized administrator. Subjects are uniquely identified by the PIX Firewall by using PIX interface, source IP address, destination IP address, port, and sequence numbers. Using the connection information, the ASA maintains domain separation.

There are two objects maintained by the TOE to support connections between hosts. They are the CONNECTION entry and the XLATE entry. CONNECTION entries maintain all information needed to manage a connection (or session) between two hosts. After the ASA determines that a requested connection between two hosts satisfies the security policy established by the PIX firewall administrator, a CONNECTION entry is allocated to manage that connection. When a connection between two hosts is terminated, the associated CONNECTION entry is de-allocated and returned to the pool of available resources.

XLATE entries maintain information about the association between two distinct hosts that have active connections through the PIX. An XLATE entry is allocated when a new connection is established between two hosts, and no other connections between them

exist. The CONNECTION entries associated with subsequent connections between a distinct pair of hosts are linked to their XLATE entry. When the last connection between two hosts is terminated (and the associated CONNECTION entry is de-allocated), the XLATE entry associating those two hosts is de-allocated.

Conclusion. The TOE satisfies the FPT\_SEP.1 requirements.

#### **7.4.11 FPT\_STM.1 Reliable timestamps**

##### Requirement

FPT\_STM.1.1 - The TSF shall be able to provide reliable timestamps for its own use.

##### Applicable Features

This PIX Firewall inserts a timestamp at the beginning of each generated syslog messages. The timestamp is fetched from the real time stored in the PIX Firewall motherboard. The NT Workstation uses the clock on its motherboard to generate timestamps for event log records. The syslog messages generated on the PIX Firewall are sent to the NT Workstation and stored in log files. These log files are translated into a format to be reviewed using Microsoft Access. The syslog messages and event log messages are never combined such that ordering of the occurrence of events within the event log and the log files is preserved and not potentially misinterpreted.

Conclusion. The TOE satisfies the FPT\_STM.1 requirement.

#### **7.4.12 FAU\_GEN.1 Audit data generation**

##### Requirement

FAU\_GEN.1.1 - The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shut down of the audit functions
- b) All relevant auditable events for the minimal or basic level of audit specified in Table 5.2<sup>6</sup>
- c) [the event in Table 5.2 listed at the "extended" level]

---

<sup>6</sup> Table 5.2 is shown in this report as Figure 3

FAU\_GEN.1.2 - The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subjects identities, outcome (success or failure) of the event
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, information specified in column four of Table 5.2.

Functional Component	Level	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	minimal	Modifications to the group of users that are part of the authorized administrator role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role.
FIA_UID.2	basic	All use of the user identification mechanism.	The user identities provided to the TOE.
FIA_UAU.1	basic	Any use of the authentication mechanism.	The user identities provided to the TOE.
FIA_AFL.1	minimal	The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the authorized administrator of the users capability to authenticate.	The identity of the offending user and the authorized administrator.
FDP_IFF.1	basic	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FCS_COP.1	minimal	Success and failure, and the type of cryptographic operation.	The identity of the external IT entity attempting to perform the cryptographic operation.
FPT_STM.1	minimal	Changes to the time.	The identity of the authorized administrator performing the operation.
FMT_MOF.1	extended	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation.

**Figure 3 Auditable Events**

### Applicable Features

Because the evaluated configuration of the TOE is not configured to support remote administration and authorized external IT entities, the TOE does not audit the FIA\_AFL.1 and FCS\_COP.1 audit events. The TOE can generate 12 different types of audit events. These events include startup and shutdown of audit functions, actions taken by the administrator, identification and authentication, and decisions on requests for information

flow. A complete list of event types is presented in Table 6. For each event, the audit record includes date and time of the event, type of event, and the process ID that generated the audit record. The success or failure of the event is indicated in the event description or implied by the type of event. Events for actions taken by the administrator include the identity of the administrator. Also, for the modification to the administrator role event, the user identity being modified is recorded. User identities provided to the TOE are included for identification and authentication events. The presumed source and destination addresses are included in audit events relating to decisions on requests for information flow.

**Table 6 TOE Audit Events**

<b>Audit Event</b>	<b>Generated by</b>
Startup of Event Log	The NT Event Log is active on the NT Workstation at all times unless disabled at startup.
Startup and Shutdown of PFSS	The PFSS captures its startup in the pfss.log.
Modifications to the group of users that are part of the authorized administrator role	The User Manager of the NT Security Subsystem generated events when modifications to administrator roles are made.
All use of the user identification mechanism, including the user identity provided	The user identification mechanism is the NT security subsystem. The NT security subsystem records all usage in the Event Log.
All use of the authentication mechanism	The user authentication mechanism is the NT security subsystem. The NT security subsystem records all usage in the Event Log.
All decisions on request for information flow	The PIX Firewall sends Syslog messages auditing all decisions for information flow.
Startup and shutdown of the TOE	The PIX sends a Syslog message when it powers up. The NT Workstation logs startup events.
Create, delete, modify, and view information flow security policy rules that permit or deny information flows	The PIX Firewall sends a Syslog message upon each modification to the PIX configuration. This will include conduit, static, outbound, and apply

Audit Event	Generated by
	commands.
Create, delete, modify, and view user attributes	NT Event Log captures the creation of accounts and attributes.
Modify and set the time and date	The PIX Firewall generates a Syslog message when the clock command is issued. The NT Workstation captures the event with Event Log.
Archive, create, delete, review, and empty the audit trail	The NT Workstation generates an audit event when the Event log is cleared. All access to the files generated by the PFSS is audited by the NTFS Security functions.
Backup and recovery, where the backup capability shall be supported by automated tools	All back up and recovery of the audit trail data is done using the NTFS. The backup and recovery commands of the PIX Firewall are logged to the PFSS.

Conclusion. The TOE satisfies the FAU\_GEN.1 requirements.

#### 7.4.13 FAU\_SAR.1 Audit review

##### Requirement

FAU\_SAR.1.1 - The TSF shall provide an authorized administrator with the capability to read all audit trail data from the audit records.

FAU\_SAR.1.2 - The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

##### Applicable Features

As defined by the administrator role, the authorized administrator has the necessary privileges to read the audit trail event log and syslog files. The TOE provides the Event Viewer and Microsoft Access as the mechanisms to review the event log and syslog files, respectively. The administrator must use the pfssfmt and logfmt utilities to convert the syslog files into a Microsoft Access format. Use of these utilities is described in *Cisco PIX Firewall 520 Version 4.3(1) Administrative Guidance White Paper*.

Conclusion. The TOE satisfies the FAU\_SAR.1 requirements.

#### **7.4.14 FAU\_SAR.3 Selectable audit review**

##### Requirement

FAU\_SAR.3.1 - The TSF shall provide the ability to perform searches and sorting of audit data based on:

- a) presumed subject address
- b) ranges of dates
- c) ranges of times
- d) ranges of addresses

##### Applicable Features

The TOE provides the Event Viewer and Microsoft Access as the mechanisms to search and sort the event log and syslog files, respectively. Event Viewer allows searching and sorting based on date and time. IP addresses are not supported because the audit records captured by the Event log do not include IP addresses. The administrator must use the pfssfmt and logfmt utilities to convert the syslog files into a Microsoft Access format. Microsoft Access provides a searching and sorting capability based on IP addresses, dates, and times. The *Cisco PIX Firewall 520 Version 4.3(1) Administrative Guidance White Paper* provides sample Microsoft Access queries to use for searching and sorting.

Conclusion. The TOE satisfies the FAU\_SAR.3 requirement.

#### **7.4.15 FAU\_STG.1 Protected audit trail storage**

##### Requirement

FAU\_STG.1.1 - The TSF shall protect the stored audit records from unauthorized deletion.

FAU\_STG.1.2 - The TSF shall be able to prevent modifications to the audit records by users other than an authorized administrator.

##### Applicable Features

The TOE protects the audit records stored in the event log and syslog files by using Windows NT secure files system called NTFS. At user logon, Windows NT generates an access token for the user. The win32 subsystem uses that token to determine the user's access to all files on the NTFS disk. If the user does not belong to a group that has permission to access a file then NTFS denies the user access. All the syslog files and event log are protected by NTFS. Only users belonging to the administrator group can access and manipulate these files. The only users allowed on the NT workstation are the

authorized administrators, and authorized administrators are the only users that can modify, archive, and delete audit records.

Conclusion. The TOE satisfies the FAU\_STG.1 requirements.

#### **7.4.16 FAU\_STG.4 Prevention of audit data loss**

##### Requirement

FAU\_STG.4.1 - The TSF shall prevent auditable events, except those taken by the authorized administrator and shall limit the number of audit records lost if the audit trail is full.

##### Applicable Features

The TOE allows the administrator to set a disk full parameter for the PFSS. The PFSS checks this parameter periodically as defined by the administrator. If the hard disk is found to have exceeded the disk-full parameter threshold, the PFSS closes its TCP connection to the PIX Firewall. The PIX Firewall will try to reconnect up to five tries. If the connection cannot be reestablished, the PIX Firewall will not allow any new connections to be established, and data traffic for existing connections will be shut down. The administrator will be able to continue performing actions and is audited up until the actual hard disk space on the NT Workstation becomes full. If the administrator sets a threshold such that the disk full parameter is set to a reasonable limit below an actual hard disk full limit, no audit data will be lost. Once the disk space is free again, the PFSS will start listening for incoming connections from the PIX Firewall. The administrator must manually reconfigure the PIX Firewall to restore the TCP connection with the NT Workstation.

Conclusion. The TOE satisfies the FAU\_STG.4 requirement.

#### **7.4.17 FMT\_MOF.1 Management of security functions behavior**

##### Requirement

FMT\_MOF.1.1 - The TSF shall provide and restrict the ability to perform the following functions to an authorized administrator:

- a) startup and shutdown
- b) create, delete, modify, and view information flow security policy rules that permit or deny information flows
- c) create, delete, modify, and view user attribute values defined in FIA\_ATD.1

- d) enable and disable single-use authentication mechanisms in FIA\_UAU.4 (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network)
- e) modify and set the threshold for the number of permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network)
- f) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network)
- g) enable and disable external IT entities from communicating to the TOE (if the TOE supports authorized external IT entities)
- h) modify and set the time and date
- i) archive, create, delete, empty, and review the audit trail
- j) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools
- k) recover to the state following the last backup
- l) additionally, if the TSF supports remote administration from either an internal or external network:
  - enable and disable remote administration from internal and external networks
  - restrict addresses from which remote administration can be performed
- m) no additional operations

### Applicable Features

Because the evaluated TOE is not configured to support remote administration and authorized external entities, the following FMT\_MOF.1 items were not applicable for this evaluation: (d), (e), (f), (g), and (l). The TOE provides and restricts the ability to perform the following functions to the administrator:

- Start up and shutdown – This is restricted by the physical environment such that only authorized administrators are allowed to access the TOE.

- Administer information flow rules – The PIX Firewall requires the administrator to authenticate himself or herself before changing the configuration file on the PIX Firewall. The administrator uses the `outbound/apply` and `conduit/static` commands to create, modify, and delete flow rules. The `show config` command allows the administrator to view the flow rules.
- Administer user accounts – The User Manager of the Windows NT allows the administrator to create, delete, modify, and view user accounts.
- Modify and set the time and date - Both the PIX Firewall and the NT Workstation maintain their own clocks. To modify the PIX Firewall clock, the administrator must authenticate himself or herself before using the `clock set` command. To modify the NT Workstation clock, the Date and Time applet in the Control Panel is used.
- Administering the audit trail - The audit trail is maintained on the NT Workstation in the event log and the syslog files. The event log is reviewed by using Event Viewer. The syslog files are reformatted using the `pfssfmt` and `logfmt` utilities and imported into Microsoft Access for review. The event log and syslog files can be deleted and copied (i.e., archive) by using the standard NTFS file commands. The administrator does not explicitly create the audit trail; the event log service and PFSS create the audit trail.
- Backup and recovery - Backup and recovery is a function of the native utilities on both the NT Workstation and the PIX Firewall. Windows NT backup and recovery functions are used to write to and read from the tape drive user attribute files and audit trail. PIX Firewall backup and recovery commands are used to write to and read from floppy disk the configuration file.

Conclusion. The TOE satisfies the FMT\_MOF.1 requirement.

## **8.0 Evaluator Comments**

### **8.1 Audit Review Tool**

The FAU\_SAR.3 requirement requires a search and sorting tool to be provided by the TOE. Third-party tools (Event Viewer and Microsoft Access) were included in the definition of the TOE just to satisfy this requirement. Because the audit records generated by the TOE are presented in a recognizable format, the need for a search and sorting tool is to aid the administrator. The evaluation team believes that the developer should have been allowed to allocate this requirement to the IT security environment since the requirement describes a user-friendly feature versus a security function. As long as the TOE generates the audit records in a format that is readable and understandable, a consumer of the TOE should be able to select their choice of a search and sorting tool.

### **8.2 Auditable Events**

The TOE audits all actions of the authorized administrator, which is more than required by the FAU\_GEN.1 requirements.

### **8.3 TOE Architecture**

The TFFPP assumes a monolithic architecture (i.e., all components of the TOE reside in the same physical device). However, most traffic-filter firewalls follow a distributed model, with the SFP enforcing component physically separate from the administrator support component. In addition, firewall implementations are usually applications executing on top of a COTS operating system and hardware environment and may rely on the underlying environments protection features. Because the TFFPP is written such that all SFRs must be allocated to the TOE, the developer was forced to include components outside their control in their definition of the TOE. The evaluation team believes that the developer should have been allowed to allocate those SFRs which don't enforce the SFP to the IT security environment.

### **8.4 Asymmetric Rules for Policy Enforcement**

The rules for enforcing the policy for inbound connections are different than for outbound connections. Likewise, the commands used to specify the policy for inbound connections are different than for outbound connections. Configuring the security policy for the PIX Firewall is non-trivial. The administrator must be aware of these differences to properly configure the desired security policy.

### **8.5 Use of Procedures to Avoid Contradictory Audit Message**

As part of installation and generation, two conduit rules are defined to prevent contradictory audit messages from being generated when packets arrive on one interface with a source address on the destination network. The evaluation team believes that this is a work around and should be fixed within the software image as opposed to configuration rules.

## 9.0 Glossary

<b>CC</b>	Common Criteria for Information Technology Security Evaluation
<b>EAL</b>	Evaluation Assurance Level
<b>IT</b>	Information Technology
<b>PP</b>	Protection Profile
<b>SFP</b>	Security Function Policy
<b>ST</b>	Security Target
<b>TFFPP</b>	Traffic-Filter Firewall Protection Profile
<b>TOE</b>	Target of Evaluation
<b>TSC</b>	TSF Scope of Control
<b>TSF</b>	TOE Security Functions
<b>TSP</b>	TOE Security Policy

## 10.0 Bibliography

This section contains all the referenced documentation used as source material in the compilation of this report.

Vendor supplied documentation:

- *Cisco PIX Firewall 520 Version 4.3(1) Administrative Guidance White Paper*, Version 1.0
- *Cisco PIX Firewall 520 Version 4.3.(1) Correspondence White Paper*, Version 1.0
- *Cisco PIX Target of Evaluation Test Procedures Document*, Version 1.0
- *Cisco PIX Firewall 520 Version 4.3(1) Security Target, Version 1.2*, December 1998
- *Cisco PIX Firewall 520 Version 4.3(1) Installation and Configuration White Paper*, Version 1.0
- *Configuration Management and Delivery Document*, Version 1.0
- *Configuration Guide for the PIX 4.2*
- *Hardware Functional Specification (Lego) Revision 1.2*
- *NT Workstation Architecture Document*, Version 1.0
- *PIX Firewall Quick Installation Guide 4.2*
- *PIX Firewall Syslog Server White Paper*, Version 2.3
- *PIX V4.3.1 Architecture and Detailed Design*, Version 1.2
- *Release Notes for the PIX Firewall 4.2*
- *System Log Messages for the PIX Firewall*, Version 4.2

Criteria and TTAP Program documentation:

- *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model*, Version 2.0, CCIB-98-026, May 1998
- *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements*, Version 2.0, CCIB-98-027, May 1998
- *Common Criteria for Information Technology Security Evaluation, Part 2: Annexes*, Version 2.0, CCIB-98-027A, May 1998
- *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements*, Version 2.0, CCIB-98-028, May 1998
- *Proposed TTAP Process for Common Criteria EAL 1&2 Evaluations*, January 1998
- *TTAP Scheme, Version 1.1*, November 1997

- *U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments; Version 1.a, August 1998*
- *U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments; Version 1.c, November 1998*

Technical reference:

- *Common Criteria Testing Program Derived Test Requirements of the U.S. Government Traffic Filter Firewall Protection Profile for Low Risk Environments, Version 1.0, April 1998*

## **Appendix A – Security Target**

*(Attach Cisco PIX Firewall 520 Version 4.3(1) Security Target, Version 1.2, December 1998)*

## Appendix B - Evaluated Configuration Parameters and Files

The evaluated TOE test configuration network had the following IP addresses and network masks assigned:

- Assigned network address: 1.2.2.0; subnet mask: 255.255.255.192
- Outside network interface address: 1.2.2.1, network mask: 255.255.255.192
- Allowable global and static addresses on the outside network: 1.2.2.1 – 1.2.2.63
- Inside network interface address: 1.0.0.1, network mask: 255.255.255.255
- Allowable global and static addresses on the inside network: 1.0.0.1 – 1.0.0.254
- NT Workstation network interface address: 10.1.1.1, network mask: 255.255.255.252
- Allowable global and static addresses on the NT Workstation network: 10.1.1.1 – 10.1.1.2

Configuration file for default TOE configuration. This configuration is created as a result of the following the installation and generation instructions in *Cisco PIX Firewall 520 Version 4.3(1) Installation and Configuration White Paper*:

```
PIX Version 4.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 admin security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address admin 0.0.0.0
names
no pager
logging timestamp
no logging console
no logging monitor
no logging buffered
logging trap debugging
logging facility 20
logging host admin 10.1.1.2 6/1468
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
ip address outside 1.2.2.1 255.255.255.192
ip address inside 1.0.0.1 255.255.255.0
```

```
ip address admin 10.1.1.1 255.255.255.252
arp timeout 14400
nat (inside) 0 1.0.0.0 255.255.255.0 100 100
conduit deny ip any 1.0.0.0 255.255.255.0
conduit deny ip any 10.1.1.0 255.255.255.252
outbound 1 deny 0.0.0.0 0.0.0.0 0 ip
apply (inside) 1 outgoing_src
apply (inside) 1 outgoing_dest
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
no rip admin passive
no rip admin default
timeout xlate 3:00:00 conn 1:00:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
tacacs-server (admin) host 10.1.1.2 aceface7 timeout 5
aaa authentication any console tacacs+
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
telnet timeout 5
mtu outside 1500
mtu inside 1500
mtu admin 1500
floodguard 9
fragguard
sysopt security fragguard
sysopt connection enforcesubnet
Cryptochecksum:154c39152fee59ffclabaa15daf6bcf2
```

#### Configuration file for Outbound-Only flows:

```
PIX Version 4.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 admin security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address admin 0.0.0.0
names
no pager
logging timestamp
```

```
no logging console
no logging monitor
no logging buffered
logging trap debugging
logging facility 20
logging host admin 10.1.1.2 6/1468
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
ip address outside 1.2.2.1 255.255.255.192
ip address inside 1.0.0.1 255.255.255.0
ip address admin 10.1.1.1 255.255.255.252
arp timeout 14400
nat (inside) 0 1.0.0.0 255.255.255.0 100 100
conduit deny ip any 1.0.0.0 255.255.255.0
conduit deny ip any 10.1.1.0 255.255.255.252
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
no rip admin passive
no rip admin default
timeout xlate 3:00:00 conn 1:00:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
tacacs-server (admin) host 10.1.1.2 aceface7 timeout 5
aaa authentication any console tacacs+
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
telnet timeout 5
mtu outside 1500
mtu inside 1500
mtu admin 1500
floodguard 9
fragguard
sysopt security fragguard
sysopt connection enforcesubnet
Cryptochecksum:154c39152fee59ffclabaa15daf6bcf2
```

#### Configuration file for Two-Way traffic:

```
PIX Version 4.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 admin security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
```

```
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address admin 0.0.0.0
names
no pager
logging timestamp
no logging console
no logging monitor
no logging buffered
logging trap debugging
logging facility 20
logging host admin 10.1.1.2 6/1468
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
ip address outside 1.2.2.1 255.255.255.192
ip address inside 1.0.0.1 255.255.255.0
ip address admin 10.1.1.1 255.255.255.252
arp timeout 14400
nat (inside) 0 1.0.0.0 255.255.255.0 100 100
conduit deny ip any 1.0.0.0 255.255.255.0
conduit deny ip any 10.1.1.0 255.255.255.252
conduit permit tcp 1.0.0.4 255.255.255.255 eq www 1.2.2.0 255.255.255.192
static (inside,outside) 1.0.0.4 1.0.0.4 netmask 255.255.255.255
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
no rip admin passive
no rip admin default
timeout xlate 3:00:00 conn 1:00:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
tacacs-server (admin) host 10.1.1.2 aceface7 timeout 5
aaa authentication any console tacacs+
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
telnet timeout 5
mtu outside 1500
mtu inside 1500
mtu admin 1500
floodguard 9
fragguard
sysopt security fragguard
sysopt connection enforcesubnet
Cryptochecksum:154c39152fee59ffclabaa15daf6bcf2
```